UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,472	01/26/2001	Jean Louis Calvignac	RAL920000119US1	6208

25299 7590 03/28/2007

IBM CORPORATION
PO BOX 12195
DEPT YXSA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	03/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/771,472
Filing Date: January 26, 2001
Appellant(s): CALVIGNAC ET AL.

Andrew M. Calderon
Reg. No. 38,093
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 20 December 2006, appealing from the Office action mailed 13 June 2006.

(1) Real Party in Interest

The real party in interest is International Business Machines Corporation by an assignment recorded in the U.S. Patent and Trademark Office on January 26, 2001, at Reel 011498 and Frame 0541.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner: Claim Rejection 35 USC §112, second paragraph placed on claims 9, 11, 13, and 17-20 is removed.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

U.S. Patent No. 6,870,929 to Greene, issued March 22, 2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-20 are rejected under 35 § U.S.C. 102(e) as being anticipated by Greene U.S. Patent No. 6,870,929 (hereinafter '929).

Regarding claim 1, as per the first limitation **"A hardware implementation of a crypto-function comprising: a first register storing data to be encrypted or decrypted;"** is taught in '929 col. 4, lines 6-31 "According to one embodiment, an encryption system can include an input buffer that receives data blocks ... While the term "encryption" is used throughout this description, it is understood that "encryption" can include both encryption and decryption";

As per the second limitation, **"a second register for receiving data which has been encrypted or decrypted"** is shown in '929 col. 5, lines 1-5 "Referring now to FIG. 1, a block diagram is set forth illustrating a first embodiment. The first embodiment is designated by the general reference character 100, and is shown to include an encryption circuit 102, an input buffer/working store 104, an output buffer 108, and a scheduler 106";

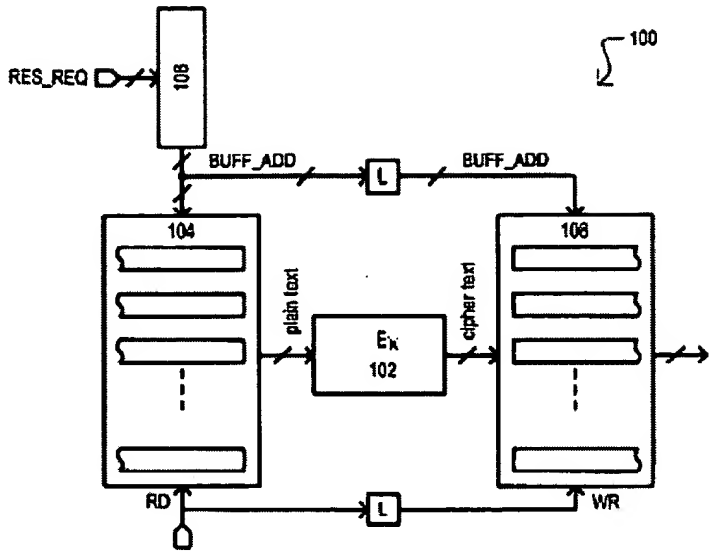

FIG. 1

As per the third limitation, **"and combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle"** is disclosed in '929 col. 5, lines 6-12 "An encryption circuit 102 can include a number of cipher stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L, where L=nT. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stag" (Note "combinational logic performing computation iteration of the crypto-function" is interpreted to have the same meaning as 'a number of cipher stages", also note "a single hardware cycle" is interpreted to have the same meaning as 'an encryption circuit').

Regarding claim 2, as per the first limitation **"wherein the crypto-function is a block cipher algorithm"** is taught in '929 col. 6, lines 58-67 "An encryption circuit 102 can also be capable of "feedback"-type encryption functions, such as cipher block chaining (CBC), cipher feedback (CFB) or output feedback (OFB) modes of the data encryption algorithms such as DES

and Triple DES, or any of various secure hash algorithms. In such an arrangement, consecutive blocks from a context can be applied a predetermined latency from one another, where the predetermined latency is that of the encryption circuit. For example, in a DES CBC mode, a latency can be one pass through an encryption pipeline".

Regarding claim 3, as per the first limitation **"wherein the crypto-function is the Data Encryption Standard (DES) algorithm"** is shown in '929 col. 6, lines 58-67.

Regarding claim 4, as per the first limitation **"wherein the crypto-function is the CHAIN algorithm"** is disclosed in ''929 col. 6, lines 58-67.

Regarding claim 5, as per the first limitation **"wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times"** is taught in '929 col. 7, lines 7-21 and col. 7, line 62 through col. 8, line 4 "In FIG. 4A, data blocks from different contexts are given a particular letter designation and number designation. The letter designation indicates a context of origin, the number designation indicates how many blocks have previously been processed for the context in question. Thus, a first context can provide data block A1, followed by data block A2, followed by data block A3, etc. Further, if it is assumed that CBC is employed, the encrypted form of data block A1 (designated as E[A1]) is an input that is used together with data block A2 to encrypt data block A2. In general, each context will have its own encryption/decryption key (or, in the case of Triple-DES and similar algorithms, set of encryption/decryption keys). The keys for all active contexts are stored and retrieved at appropriate times as seen below" and "A scheduler 106 can be programmed to provide appropriate priority to ensure feedback-type encryption operations. In particular, the active contexts can be stored, and on consecutive cycles, priority can be shifted to

give the desired context priority. As shown in FIG. 4A, at time t14, priority can be shifted to give data block E1 priority. Further, one skilled in the art would recognize that the feedback loop in an encryption circuit would be disabled on this cycle to prevent the E_{KB} [B3] value from being combined with the E1 value".

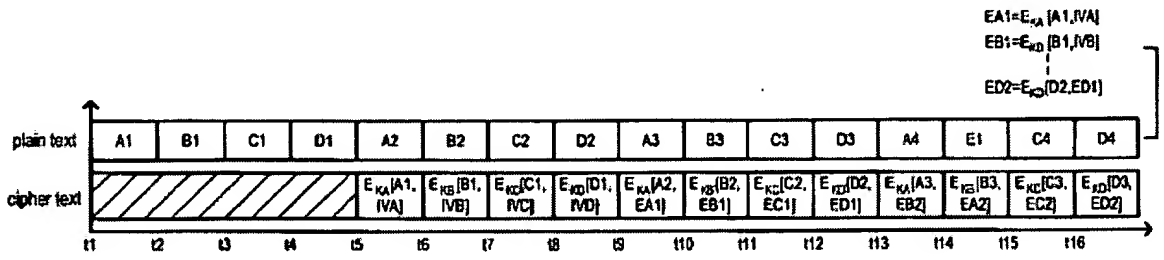

FIG. 4A

Regarding claim 6, as per the first limitation **"wherein the combinational logic performs mixing, permutation and key-dependent substitution in each round"** is shown in '929 col. 7, lines 7-21 and col. 8, lines 6-32 "In an alternate embodiment, a system may include as many contexts as there are pipeline stages. Each context can be accessed sequentially. In the event a context does not include a data block, a read from the input buffer and write to the output buffer can be suppressed. In this way, an encryption system can provide an encrypted data block in each system cycle for feedback-type encryption. This is in contrast to a conventional approach that may supply a first data block of a sequence to an encryption circuit and then supply the second block a predetermined time later, limited by the latency of the encryption process on the first data block. Thus, the present invention can process a data block on each system cycle (provided sufficient contexts are active) even when the encryption function includes a feedback loop. While the above description has described the particularly useful application of the invention to encryption, the described embodiments could also be utilized in other computations,

such as modular exponentiation, as but one example. As one very particular example, if the method described in the background above is employed to compute $y=(A^e) \bmod n$, a modular multiply computation circuit (in place of the encryption circuit 102) could provide the yy=(yy*aa) mod n operation and/or the aa=(aa*aa) mod n operation. Of course, the scheduler operation could be adjusted to ensure that the yy=(yy*aa) mod n operation is performed only for iterations corresponding to an "e" bit value equal to one".

Regarding claim 7, as per the first limitation **"wherein the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation"** is disclosed in '929 col. 7, lines 51-67 "A scheduling section 502 can include a register array 510 having n rows and m columns. The variable n can be the number of contexts in an input buffer/working store 504. As but one example, n rows can correspond to n FIFO pipelines storing data blocks for encryption. The variable m can be the number of parallel encryption circuits within encryption section 506, where each encryption circuit is capable of processing one data block per m cycles, such that encryption section 506 can process in aggregate one data block per cycle. The various rows of the register array 510 can be loaded on a row-by-row basis by operation of load circuit 512. The load circuit 512 may load a row of the register array 510 according to a current address (ADD_CURR) and current data (DATA_CURR) or alternatively, according to a next address (ADD_NXT) and next data (DATA_NXT).".

Regarding claim 8, as per the first limitation **"wherein the combinational logic deciphers a block by performing deciphering using the same key as used to encipher the**

block in a process that is an inverse of the enciphering process" is taught in '929 col. 10, lines 8-17 "Scheduling, such as that described in conjunction with FIGS. 4A and 4B can be used to accomplish pipelined feedback-type encryption operations. One particular feedback structure is set forth in FIG. 5. A feedback bus 528 can couple output buffer 508 data to a combining circuit 530 (in this particular example an XOR circuit). In the case of a feedback-type algorithm, a read operation can be performed on the output buffer 508. The read data (which can be a previously encrypted data block) can then be combined with an "incoming" data block in combining circuit 530".

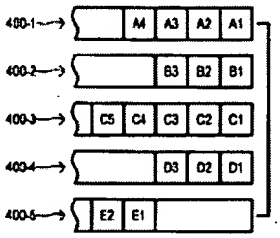

FIG. 4B

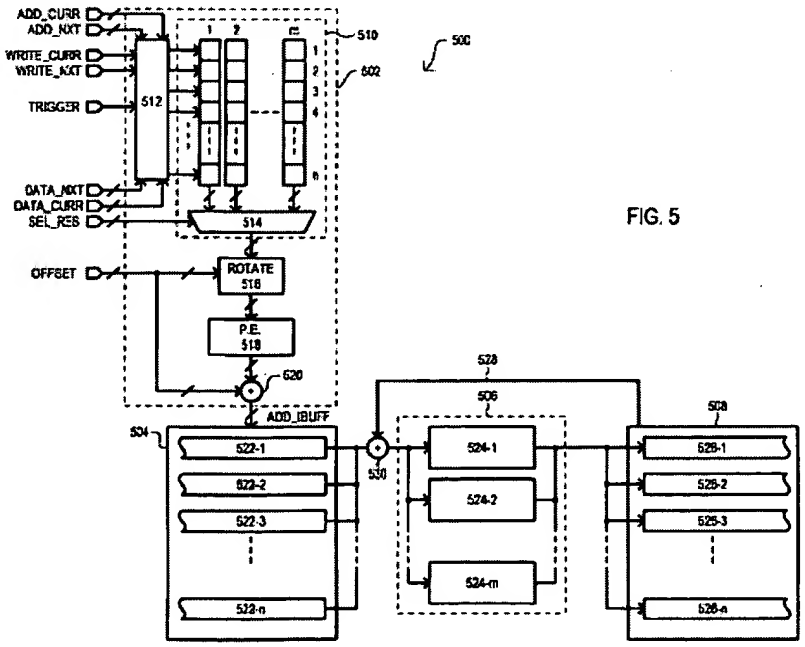

FIG. 5

Regarding claim 9, as per the first limitation **"wherein the one hardware cycle is approximately ten clock cycles"** is shown in '929 col. 5, lines 7-12 "An encryption circuit 102 can include a number of cipher stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L, where L=nT. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage".

Regarding claim 10, as per the first limitation **"wherein the hardware implementation of the crypto-function uses only the combinational logic without having to store intermediate results in registers"** is disclosed in '929 col. 4, lines 58-67 "Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit".

Regarding claim 11, as per the first limitation **"wherein the hardware implementation the crypt-function computes an iterated round function in one clock cycle"** is taught in '929 col. 5, lines 7-12.

Regarding claim 12, as per the first limitation **"wherein the combination logic utilizes a Data Encryption Standard (DES) algorithm that is implemented in the combination logic"** is shown in '929 col. 6, lines 58-67.

Regarding claim 13, as per the first limitation **"wherein the combination logic utilizes logic functions whose outputs depend solely on their inputs"** is disclosed in '929 col. 5, lines 12-23 "The input buffer/working store 104 can include various storage circuits that store data blocks from multiple data streams. Each data stream can include one data block, or a sequence of data blocks having a particular order. Each such data block and/or sequence of data blocks will be referred to herein as a "context." As just one example, each context can represent data from a particular network packet. An input buffer/working store 104 can be implemented in a variety of forms. As but two of the many possible examples, and input buffer can include first-in-first-out (FIFO) memory device(s) or random access memory (RAM) device(s)."

Regarding claim 14, as per the first limitation **"wherein the combination logic utilizes logic circuits without memory, whereby no registers are used to store intermediate results or iterations of encipher or deciphering computations"** is taught in '929 col. 4, lines 29-67.

Regarding claim 15, as per the first limitation**, "wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read"** is shown in '929 col. 4, lines 58-67.

Regarding claim 16, as per the first limitation **"A hardware implementation of a crypto-function comprising: a first register that stores data to be encrypted or decrypted; a second register that receives data which has been encrypted or decrypted; and combinational logic that performs computation iteration of the crypto-function on data store in the first register"** is taught in '929 col. 4, lines 6-31;

As per the second limitation, **"and outputting data to said second register"** is shown in '929 col. 5, lines 1-5;

As per the third limitation, **"in a single hardware cycle, wherein the crypt-function"** is disclosed in '929 col. 4, lines 58-67;

As per the fourth limitation, **"is implanted in the combination logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read"** is taught in '929 col. 5, lines 6-12 (Note "combinational logic performing computation iteration of the crypto-function" is interpreted to have the same meaning as 'a number of cipher stages", also note "a single hardware cycle" is interpreted to have the same meaning as 'an encryption circuit').

Regarding claim 17, as per the first limitation **"wherein the single hardware cycle is approximately ten clock cycles"** is disclosed in ''929 col. 4, lines 58-67.

Regarding claim 18, as per the first limitation **"wherein the hardware implementation of the crypto-function computes and iterated round in just one clock cycle"** is disclosed in ''929 col. 4, lines 58-67.

Regarding claim 19, as per the first limitation **"A hardware implementation of a crypto-function comprising: a first register that stores data to be encrypted or decrypted; a second register that receives data which has been encrypted or decrypted; and combination logic that performs computation iteration of the crypto-function on data stored in the first register"** is taught in '929 col. 4, lines 6-31;

As per the second limitation, **"and outputting data to said second register"** is shown in '929 col. 5, lines 1-5;

As per the third limitation, **"in a single hardware cycle"** is disclosed in '929 col. 4, lines 58-67;

As per the fourth limitation, **"wherein the single hardware cycle comprises several clock cycles"** is taught in '929 col. 5, lines 8-12.

Regarding claim 20, as per the first limitation, **"wherein the cypto-function is implemented in the combination logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read"** is shown in '929 col. 4, lines 58-67.

(10) Response to Argument

Regarding Appellant's argument first argument, with respect to claim 1, beginning on page 5 Applicant states that the 35 U.S.C. 102 (e) rejection with respect to US Patent No. 6,870,929 to Greene is in error because Greene does not disclose, or even suggest combinational logic performing computation iterations of the crypto-function on data stored in the first register and output to the second register in a single hardware cycle.

The grounds of rejection stand, as indicated in Final Office Actions Greene discloses 'combination logic performing computation iterations of the crypto-function on data stored in the first register and output to the second register in a single hardware cycle'. Note see col. 5, lines 1-15 as well as col. 4, lines 58-67 of Greene.

> "Referring now to FIG. 1, a block diagram is set forth illustrating a first embodiment. The first embodiment is designated by the general reference character 100, and is shown to include an encryption circuit 102, an input

buffer/working store 104, an output buffer 108, and a scheduler 106. An encryption circuit 102 can include a number of cipher stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L, where L=nT. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage."

and

"Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit"

Using the broadest reasonable interpretation, 'combination logic performing computation iterations of the crypto-function on data' equates to 'the data blocks that can be pipelined across one or more encryption circuits'. Using the broadest reasonable interpretation, 'the first register' equates to 'the input buffer'. Using the broadest reasonable interpretation, 'the second register' equates to the 'output buffer'. Using the broadest reasonable interpretation, 'in a single hardware cycle' equates to 'where a cycle can be as small as one clocked cipher stage within an encryption circuit'.

This argument is repeated in similar context with respect to claims 11, 16, and 19.

Regarding Appellant's argument second argument, with respect to independent claim 16, beginning on page 11, "The above-noted language simply does not disclose that the crypto-function is implemented in the combination logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read, and the Examiner has not demonstrated otherwise".

The grounds of rejection stand, as indicated in Final Office Actions see Greene col. 4, lines 58-67, using the broadest reasonable interpretation, 'the crypto-function is implemented in combination logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read' is equated equivalent to pipelined encryption system disclosed that indicates the delay can be as small as one clock cycle. Therefore no settling or loading would occur information would be fed into an encryption or decryption circuit.

This argument is repeated in similar context with respect to claims 10, 13-15, and 20.

Regarding Appellant's argument third argument, with respect to dependent claims 2-4, beginning on page 15, "Greene does not disclose that such algorithms can be used with, among other things the recited combination logic of claims (for the reasons noted above)".

The grounds of rejection stand, as indicated in Final Office Actions claims 2-4, are taught in Greene col. 6, lines 58-67. Note 'encryption circuit 102', is shown in col. 5, lines 7-12 as well as col. 6, lines 58-67.

This argument is repeated in similar context with respect to claims 8 and 12.

Regarding Appellant's argument fourth argument, with respect to dependent claim 5, beginning on page 17, "Greene does not disclose that such algorithms can be used with, among

other things the recited combination logic of claims (for the reasons noted above) ... the Examiner is not correct that col. 7, lines 7-21 and col. 7, line 62 to col. 8, line 4 discloses that the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times".

The grounds of rejection stand, as indicated in Final Office Action, in addition to the above claims 5, is taught in Greened col. 6, lines 58-67. Note 'encryption circuit 102', is shown in col. 5, lines 7-12 as well as col. 6, lines 58-67. In addition using the broadest reasonable interpretation, an 'invertible key-dependent round function iterated a predetermined number of times' equates to 'the scheduler programmed to provide feedback encryption operations with a $E_{KB}[b3]$'.

Regarding Appellant's argument fifth argument, with respect to dependent claim 6, beginning on page 19, "Greene does not disclose that such algorithms can be used with, among other things the recited combination logic of claims (for the reasons noted above) ... the Examiner is not correct that col. 7, lines 7-21 and col. 8, lines 6-32 discloses that the combinational logic performs mixing, permutation and key-dependent substitution in each round".

The grounds of rejection stand, as indicated in Final Office Actions, in addition to above claims 6, is taught in Greene col. 6, lines 58-67. Note 'encryption circuit 102', is shown in col. 5, lines 7-12 as well as col. 6, lines 58-67. In addition using the broadest reasonable interpretation, a 'combination of the recited algorithm permutation and key-dependent substitution in each round' equates to each round will have its own encryption/decryption key and keys are stored and retrieved at active times.

Regarding Appellant's argument sixth argument, with respect to dependent claim 7, beginning on page 20, "Greene does not disclose that such algorithms can be used with, among other things the recited combination logic of claims (for the reasons noted above) ...The Examiner also not correct that col. 7, lines 51-67 discloses that the combination logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation".

The grounds of rejection stand, as indicated in Final Office Actions, in addition to above claims 7, is taught in Greened col. 7, lines 44-67. Note 'encryption circuit 102', is shown in col. 5, lines 7-12 as well as col. 6, lines 58-67. In addition using the broadest reasonable interpretation, 'the combination logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation' equates to 'feedback type encryption with corresponding keys and initial vectors'.

Regarding Appellant's argument seventh argument, with respect to dependent claim 9, beginning on page 23, "The Examiner asserted that Greene discloses all of the features recited in this claim including, among other features, one hardware cycle of approximately ten clock cycles. Appellant respectfully disagrees and traverses this rejection ... The combination of 9 and the features of claim 1 is simply not disclosed or suggested in Greene, and the Examiner has not demonstrated otherwise".

The grounds of rejection stand, as indicated in Final Office Actions, in addition to above claims 9, is taught in Greene col. 4, lines 62-67. Note using the broadest reasonable

interpretation 'ten clock cycles' equates to 'multiple encryption circuits' and 'one hardware cycle' equates to 'one clocked cipher state'.

These arguments are repeated in similar context with respect to claims 11, 17, and 18.

Regarding Appellant's arguments on pages 24-32, with respect to claims 11-15 and 17-20; these arguments contain substantially similar context as the arguments that have been noted and answered above. In addition each response above notes when the argument is the same for a respective claim. Therefore the grounds of rejection stand.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
20 March 2007

Conferences:

Taghi T. Arani

Eddie Lee

EDDIE C. LEE
SUPERVISORY PATENT EXAMINER